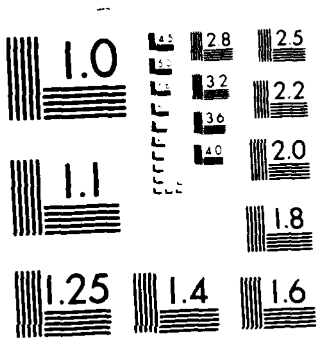
AD-A128 418 ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE MATRIX INVERSION BASE..(U) MARYLAND UNIV COLLEGE PARK COMPUTER VISION LAB E V KRISHNAMURTHY NOV 82 TR-1229 1/1

UNCLASSIFIED AFOSR-TR-83-0387 AFOSR-77-3271 F/G 12/1 NL

END
DATE
FILMED
6-83
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

AFOSR-TR- 83 - 0387

A128418

[illegible]

[illegible]

[illegible] 20742

COMPUTER SCIENCE TECHNICAL REPORT SERIES

DTIC FILE COPY

UNIVERSITY OF MARYLAND
COLLEGE PARK, MARYLAND
20742

DTIC
ELECTE
MAY 2 5 1983
S E D

83 05 2 063

Approved for public release; distribution unlimited.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER AFOSR-TR- 83 - 0387	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle) ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE MATRIX INVERSION BASED ON p-ADIC APPROXIMATION	5. TYPE OF REPORT & PERIOD COVERED TECHNICAL
	6. PERFORMING ORG. REPORT NUMBER TR-1229
7. AUTHOR(s) E.V. Krishnamurthy	8. CONTRACT OR GRANT NUMBER(s) AFOSR-77-3271
9. PERFORMING ORGANIZATION NAME AND ADDRESS Department of Computer Science University of Maryland College Park MD 20742	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS PE61102F; 2304/A2
11. CONTROLLING OFFICE NAME AND ADDRESS Mathematical & Information Sciences Directorate Air Force Office of Scientific Research Bolling AFB DC 20332	12. REPORT DATE NOV 82
	13. NUMBER OF PAGES 18
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report) UNCLASSIFIED
	15a. DECLASSIFICATION DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Parallel computation; matrix inversion; p-adic approximation.

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Newton-Schultz iterative scheme is reformulated in an algebraic setting to compute the exact inverse of a matrix (or the solution of a linear system of equations) over the ring of integers, with a high order of convergence, by using a finite segment p-adic representation of a rational. This method is divergence-free; it starts with the inverse of a given matrix over a finite field (called the priming step) and then iterates successively to construct, in parallel, the p-adic approximants (Hensel Codes) of the rational elements of the inverse matrix. The p-adic approximant is then converted back (CONTINUED)

DD FORM 1 JAN 73 1473

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ITEM #20, CONTINUED: to the equivalent rational using the extended Euclidean algorithm.

The method involves only parallel matrix multiplications and complementations and has a quadratic convergence rate. Extension to achieve higher order convergence is straightforward if parallel matrix arithmetic facilities for higher precision operands (in a prime base system) are available.

- / -

TR-1229
AFOSR-77-3271

November 1982

ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE MATRIX INVERSION BASED ON p-ADIC APPROXIMATION

E. V. Krishnamurthy*

Computer Vision Laboratory
Computer Science Center
University of Maryland
College Park, MD 20742

ABSTRACT

The Newton-Schultz iterative scheme is reformulated in an algebraic setting to compute the exact inverse of a matrix (or the solution of a linear system of equations) over the ring of integers, with a high order of convergence, by using a finite segment p-adic representation of a rational. This method is divergence-free; it starts with the inverse of a given matrix over a finite field (called the priming step) and then iterates successively to construct, in parallel, the p-adic approximants (Hensel Codes) of the rational elements of the inverse matrix. The p-adic approximant is then converted back to the equivalent rational using the extended Euclidean algorithm.

The method involves only parallel matrix multiplications and complementations and has a quadratic convergence rate. Extension to achieve higher order convergence is straightforward if parallel matrix arithmetic facilities for higher precision operands (in a prime base system) are available.

*Permanent address: Indian Institute of Science, Bangalore - 560012, INDIA

The support of the U.S. Air Force Office of Scientific Research under Grant AFOSR-77-3271 is gratefully acknowledged, as is the help of Janet Salzman in preparing this paper.

1. Introduction

Error-free direct methods for the inversion of numerical and polynomial matrices are available in the literature [1] [2]. In this paper we describe a parallel error-free high-order convergent matrix inversion method for matrices over integers, based on the Newton-Schultz iterative scheme [3] [4] and the p-adic approximation [5-9]. Some of the important aspects of this scheme are:

(i) Inversion of matrices over p-adic fields, analogously to inverting or reciprocating the numbers, without any convergence problem.

(ii) The exact and simultaneous determination of the rational elements of the inverse matrix in p-adic digit parallel fashion with a quadratic or higher rate.

(iii) Easy realization of the scheme and its variants (higher-order convergent extensions) by parallel matrix multiplications.

This paper is organized in seven sections. In the second section we outline the principle of the Newton-Schultz scheme for reciprocating numbers. The third section describes the reformulation of the Newton-Schultz scheme in an algebraic setting to compute the p-adic approximant to the inverse of a matrix over the ring of integers. In the fourth section we describe the extended Euclidean algorithm that converts a given p-adic approximant over a range of rationals into an equivalent rational. The fifth section contains an example.

In Section 6 we briefly deal with the solution of a linear system of equations, having a linear convergence rate. Several remarks pertaining to possible extensions and generalizations are provided in the last section.

2. The principle

Let f(x) be a real function of the real variable x and $x=\alpha$ be a root of $f(x)=0$. We assume that:

(a) $f(x)$, $f'(x)$ and $f''(x)$ are continuous in a neighborhood $[a,b]$ of $x=\alpha$; (b) $x=\alpha$ is an isolated root in $[a,b]$; (c) $f'(x)$ and $f''(x)$ do not vanish in $[a,b]$. The search for the root $x=\alpha$ entails finding the root of the equation

$$x = x - \frac{f(x)}{f'(x)} \equiv \phi(x) .$$

Since $\phi'(\alpha)=0$ there exists a neighborhood of $x=\alpha$ such that the sequence $\{x_i\}_{i\geq 0}$ defined by

$$x_n = x_{n-1} - f(x_{n-1})/f'(x_{n-1}) \quad (n=1,2,\ldots) \tag{1}$$

converges to $x=\alpha$ if the first approximation $x=x_0$ lies in this neighborhood. Applied to the function $f(x)=1/x-a$ (1) gives the Newton-Schultz scheme

$$x_n = x_{n-1}(2-ax_{n-1}) \tag{2}$$

The sequence (2) converges to a^{-1}. The matrix inversion algorithm to be described in the next section is by analogy based on the sequence of iterates defined by (2) [3] [4].

3. The Newton-Schultz method

Let $A=[a_{ij}]$ be a matrix over the ring of integers Z and p a prime such that det A mod $p \neq 0$. (The reason for this will become clear later.) The algorithm first constructs A^{-1} mod p and using this in the Newton-Schultz recurrence obtains a segmented p-adic representation of the inverse matrix [5-9].

Theorem 1: There exists a matrix sequence $\{B_{2^i}\}_{i \geq 0}$ such that $AB_{2^i} \bmod p^{2^i} = I$ for all $i \geq 0$, where A is the matrix to be inverted and I is the identity matrix; B_{2^i} is the inverse of A(in Z) mod p^{2^i} (or B_{2^i} is the p-adic approximant of A^{-1}).

Proof: We show the sequence $\{B_{2^i}\}_{i \geq 0}$ can be generated recursively and then prove by induction that it has the property stated, namely, $AB_{2^i} \bmod p^{2^i} = I$. The first member of the sequence B_1 is obtained in a priming step by solving

$$AB_1 \bmod p = I$$

by Gaussian elimination or some other method. It amounts to finding the inverse of A in Z mod p. Then in a powering step we use the recurrence relation

$$B_{2^i} = B_{2^{i-1}} (2I - AB_{2^{i-1}}) \bmod p^{2^i} \quad (i \geq 1) \qquad (3)$$

to construct the successive iterates.

To see that the theorem holds let $AB_{2^i} \bmod p^{2^i} = I$ be true for $i = n-1 (n \geq 1)$; then, by (3)

$$(AB_{2^n}) \bmod p^{2^n} = AB_{2^{n-1}}(2I - AB_{2^{n-1}}) \bmod p^{2^n}$$

Since $AB_{2^{n-1}} \bmod p^{2^{n-1}} = I$ by the induction hypothesis, we have

$$AB_{2^{n-1}} = I + p^{2^{n-1}} E_{n-1},$$

where E_{n-1} is the error matrix. Thus we can write

$$AB_{2^n} \bmod p^{2^n} = (I + p^{2^{n-1}} E_{n-1})(I - p^{2^{n-1}} E_{n-1}) \bmod p^{2^n}.$$

Since by construction the theorem holds for $n=0$, it is true for all $n \geq 0$ by induction.

Our algorithm first obtains B_{2^k} by iterating k times, where k is the minimum integer satisfying the inequality

$$\sqrt{\frac{p^{2^k}-1}{2}} \geq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij}^2\right)^{1/2} \tag{4}$$

This inequality ensures that the largest element of the inverse matrix lies within the range of the segmented p-adic representation of the corresponding rational [5] [8].

Let N denote a positive integer satisfying the inequality

$$N \leq \sqrt{\frac{p^{2^k}-1}{2}} \tag{5}$$

We define a finite subset F_N of the rational numbers Q as the set

$$F_N = \{\alpha = \frac{c}{d};\ 0 \leq |c| \leq N \text{ and } 0 \leq |d| \leq N\}$$

We call the set F_N the order N Farey fractions, or simply Farey rationals of order N.

If p and k are properly chosen to satisfy (4) then the rationals F_N which are mapped onto their segmented p-adic representations in B_{2^k} can be uniquely recovered using an algorithm which is based on the extended Euclidean algorithm for finding the greatest common divisor of two integers [10] [11].

Let a/b and w be the ij-th entry of A^{-1} and $B_{2}k$ respectively. Then

$$ab^{-1} \bmod p^{2^k} = w \qquad (6)$$

since b^{-1} exists mod p^{2^k}, due to the fact that det A mod $p \neq 0$.

In the following section we describe how to recover a/b given w, provided (4) is satisfied. This algorithm filters out a very small subset of rationals among which the desired rational belonging to F_N occurs. We will call the function that computes a/b given w, the EUCLID; thus EUCLID(w)=a/b.

Remark

The number k determined from (4) is generally larger than desired; so to iterate k times entails much superfluous computation. A practical method of avoiding this would be to compute EUCLID ($B_{2}k$) and EUCLID($B_{2}k+1$) starting with some reasonable k and stop as soon as they are equal. This would unambiguously determine the inverse.

4. Computation of Farey rationals using the Euclidean algorithm

The Euclidean algorithm [11] constructs three pairs of numbers (u_i, u_i'), (a_i, b_i), (t_i, t_i') for each $i=0,1,2,\ldots,k$ starting with $u_0=p^r, u_0'=0$, $a_0=w, b_0=1$ and ending when $t_i=0$, as illustrated in Table 1; here the symbol [ ] denotes the lower integral part.

Note that the q_i's here correspond to the continued fraction expansion [5] [12] of p^r/w.

It can easily be shown that the pairs (a_i, b_i) in Table 1 satisfy the following conditions [10] [11]:

Cross-product rule:

$$|a_i \cdot b_{i+1}| + |a_{i+1} \cdot b_i| = p^r \leq 2N^2+1$$

Monotonicity:

$$|a_{i+1}| \leq |a_i|, \text{ with } a_0=w, a_k=1 \tag{8}$$

$$|b_{i+1}| \geq |b_i| \text{ with } b_0=1, b_k=w^{-1} \bmod p^r \tag{9}$$

where w is such that $\gcd(w,p^r)=1$ and w^{-1} denotes the multiplicative inverse of $w \bmod p^r$.

It is now necessary to show that (i) there exists a pair (a_j, b_j) in Table 1 which satisfies the condition of a Farey rational F_N (Section 3), and (ii), such a pair is unique in the sense that there exists no other pair belonging to F_N.

To prove this, we use the fact that a_i (starting with $a_o=w$) successively decreases to 1; and b_i (starting with $b_o=1$) successively increases to w^{-1} when $\gcd(w,p^r) = 1$.

Let us assume that for some j, b_j has already increased from 1 to $|N'|$ with $|N'| \leq |N|$ and is close to $|N|$, and the corresponding a_j has already decreased from w to $|N''|$ where $|N''| > |N|$ and is close to $|N|$. Then using (7) we can prove that the succeeding pair (a_{j+1}, b_{j+1}) will have to be in F_N or in other words a pair of the form (a_{j+1}, b_{j+1}) with $|a_{j+1}| \leq N$ and $|b_{j+1}| > N$ which skips a Farey rational belonging to F_N cannot exist.

For if $|a_j| \geq N+1$ and $|b_j| \leq N$ and $|a_{j+1}| \leq N$ and $|b_{j+1}| \geq N+1$, we have $|a_{j+1} \cdot b_j| \leq N^2$. Using this in (7) we obtain $|a_j \cdot b_{j+1}| \geq N^2+1$. But we have $|a_j| \geq N+1$. Therefore $|b_{j+1}| \leq (N^2+1)/(N+1) = [N]$. Hence our assumption $|b_{j+1}| > N$ is false.

We will now show that there is only one such rational belonging to F_N. In other words, we will show that if for some j, (a_j/b_j) belongs to F_N then (a_{j+1}/b_{j+1}) cannot be in F_N. Note that the cross-product is maximum when

$$|a_j| = N, \ |b_j| = N - 1$$

$$|a_{j+1}| = N-1, \ |b_{j+1}| = N.$$

In such a case

$$|a_j \cdot b_{j+1}| + |b_j \cdot a_{j+1}| = (N-1)^2 + N^2 < 2N^2 + 1$$

would still be short of satisfying (7). Notice that for any other choice of a_j, b_j, a_{j+1}, b_{j+1} the condition (7) would be more severely violated. Also when $|a_j| = |b_j| = N$, it is not possible for $|a_{j+1}| = N$, since a_{j+1} would become zero by the algorithm in Table 1.

Thus a p-adic approximant (Hensel Code [5]) with the weight w corresponds to the rational a_j/b_j belonging to F_N and the conversion is complete.

Remarks

(i) The class of rationals generated by the above algorithm may contain a rational (in non-reduced form) whose reduced form is in F_N; but this is an invalid choice. (See example.)

(ii) If $\gcd(w, p^r) \neq 1$, the factor is taken out and the result adjusted suitably.

Example

Let $p=5$, $r=4$, and $w=448$. Hence $N \leq 17$. We now show in Table 2 the computations corresponding to Table 1 of the algorithm. The Farey rational is 11/7 (and not 5/60).

5. <u>Matrix-inversion example</u>

$$\text{Let } A = \begin{bmatrix} 1 & -1 & 2 \\ 3 & 2 & 4 \\ 0 & 1 & -2 \end{bmatrix}$$

Let p = 3:

$$|[A]|_3 = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 2 & 2 \end{bmatrix} \pmod{3}$$

$$B_2 = \begin{bmatrix} 1 & 0 & 1 \\ 6 & 7 & 2 \\ 3 & 8 & 5 \end{bmatrix} \pmod{3^2=9}$$

$$B_4 = \begin{bmatrix} 1 & 0 & 1 \\ 60 & 61 & 20 \\ 30 & 71 & 50 \end{bmatrix} \pmod{3^4=81}$$

$$B_8 = \begin{bmatrix} 1 & 0 & 1 \\ 4920 & 4921 & 1640 \\ 2460 & 5741 & 4100 \end{bmatrix} \pmod{3^8=6561}$$

$$B_{16} = \begin{bmatrix} 1 & 0 & 1 \\ 32285040 & 32285041 & 10761680 \\ 16142520 & 37665881 & 26904200 \end{bmatrix} \pmod{3^{16}=43046721}$$

We find that

$$\mathrm{EUCLID}(B_{16}) = \begin{bmatrix} 1 & 0 & 1 \\ -3/4 & 1/4 & -1/4 \\ -3/8 & 1/8 & -5/8 \end{bmatrix} = \mathrm{EUCLID}(B_8) = A^{-1}$$

Note that the inverse matrix elements are simultaneously determined in p-adic digit parallel fashion with a quadratic rate of convergence.

6. Solution of a system of linear equations by linear convergence

We now briefly consider the problem of determining the solution to a system of linear equations iteratively.

Let $Ax=b$ be a system of linear equations such that det A mod $p \neq 0$, p being a prime. Let $A=A_1$ mod p and $b_1=b$ mod p. We first solve $A_1\ x^{(1)}=b_1$ mod p by Gaussian elimination (say) and thereafter use the iterative scheme

$$x^{(k+1)} = (p\ A_1^{-1}\ M\ x^{(k)} + A_1^{-1}\ b) \bmod p^{k+1} (k=1,2,\ldots)$$

where $A=A_1-p\ M$ and M is the error matrix. We can easily show by induction that

$$(Ax^{(k)} - b) \bmod p^k = 0.$$

Then, our algorithm is formally:

Step 1 Solve $A_1\ x^{(1)}=b_1$ mod p.

Step 2 Use $x^{(k+1)}=(p\ A_1^{-1}\ M\ x^{(k)} + A_1^{-1}\ b) \bmod p^{k+1}$ to obtain the next iterate.

Step 3 If EUCLID(x^k) = EUCLID(x^{k+1}) stop; else go to 2.

Remark

Note that this scheme for the solution of linear equations has only a linear order convergence. However, it has the advantage of using only matrix-vector multiplications unlike the Newton iterative scheme where matrix-matrix multiplications are involved.

7. Concluding remarks

(i) The scheme of formula (3) gives rise to quadratic convergence. It is possible to use schemes having higher-order convergence. The following scheme, for example,

$$B_{3^n} = B_{3^{n-1}} (I + (I - B_{3^{n-1}}) (2I - AB_{3^{n-1}})) \bmod p^{3^n} \quad (10)$$

has cubic convergence.

(ii) We have assumed throughout that det A mod p $\neq 0$, but in actual computation we cannot assume this a priori. We can keep choosing one prime after another until we succeed; but this is very expensive computationally. It would be better to use the method of rank 1 update, which is as follows:

We apply our algorithm to A+V instead of A where

$$V = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} [b_1, b_2, \ldots, b_n] = ab^t \quad \text{is arbitrarily chosen.} \quad (11)$$

Finally, we use the formula

$$A^{-1} = (A+V)^{-1} + \frac{(A+V)^{-1} \; V(A+V)^{-1}}{1-b^t \; (A+V)^{-1} \; a} \quad (12)$$

to retrieve the actual inverse. This method always succeeds except when $A^{-1}=0$ over Z and A mod p=0.

(iii) It is possible to extend the scope of our algorithm for the determination of the g-inverse of a singular matrix.

(iv) The algorithm determines all the elements of the inverse matrix simultaneosly in p-adic digit parallel fashion with a quadratic or higher-order convergence rate [13].

(v) In solving a system of linear equations, we note that we have split the matrix A in a very special way, namely, $A=A_1 - p M$. We could try splitting it as in the Jacobi, Gauss-Seidel or SOR method [3]; but unfortunately, the convergence in our sense is not realizable in these cases.

(vi) We can invert polynomial matrices whose elements are in Z [2] by constructing the inverses of the matrices Z[x] mod p_i for several primes p_i and then using the Chinese Remainder Theorem to construct the actual inverse [1].

i	(u_i, u'_i)	(a_i, b_i)	q_i	(t_i, t'_i)
0	$(p^r, 0)$	$(w, 1)$	$[u_o/w]$	$(u_o - a_o q_o, u'_o - b_o q_o)$
1	$(w, 1)$	(t_o, t'_o)	$[u_1/a_1]$	$(u_1 - a_1 q_1, u'_1 - b_1 q_1)$
2	(t_o, t'_o)	(t_1, t'_1)	$[u_2/a_2]$	$(u_2 - a_2 q_2, u'_2 - b_1 q_2)$
.	..	..	..	. . . .
k	(u_k, u'_k)	$(1, w^{-1})$	$[u_k/a_k]$	$(0, (-1)^{k+1} p^r)$

Table 1

Euclidean Algorithm

i	(u_i, u'_i)	(a_i, b_i)	q_i	(t_i, t'_i)
0	(625, 0)	(448, 1)	1	(177, -1)
1	(448, 1)	(177, -1)	2	(94, 3)
2	(177, -1	(94, 3)	1	(83, -4)
3	(94, 3)	(83, -4)	1	(11, 7)
4	(83, -4)	(11, 7)	7	(6, -53)
5	(11, 7)	(6, -53)	1	(5, 60)
6	(6, -53)	(5, 60)	1	(1, -113)
7	(5, 60)	(1, -113)	5	(0, 625)

Table 2

Example of Euclidean algorithm

References

1. E. V. Krishnamurthy, Exact inversion of a rational polynomial matrix using finite field transforms, SIAM J. Appl. Math. 35, 453-464, 1978.

2. E. V. Krishnamurthy, T. M. Rao, and K. Subramanian, Residue arithmetic algorithms for computing g-inverses of matrices, SIAM J. Num. Anal. 13, 155-171, 1976.

3. J. Stoer and R. Bulrisch, An Introduction to Numerical Analysis, Springer-Verlag, 1981.

4. E. V. Krishnamurthy, Economical iterative and range-transformation schemes for division, IEEE Trans. on Computers, Vol. C-20, 470-472, 1971.

5. E. V. Krishnamurthy, T. M. Rao and K. Subramanian, Finite segment p-adic number systems with applications to exact computation, Proc. Indian Acad. Sci., Vol. 81A, pp. 58-79, February 1975.

6. E. V. Krishnamurthy, T. M. Rao, and K. Subramanian, p-adic arithmetic procedures for exact matrix computation, Proc. Indian Acad. Sci., Vol. 82A, pp. 165-175, November 1975.

7. E. V. Krishnamurthy, Matrix processors using p-adic arithmetic for exact linear computations, IEEE Trans. Computers Vol. C-26, pp. 633-639, July 1977.

8. R. T. Gregory, Error-Free Computation, Robert E. Krieger Pub. Co., Huntington, NY, 1980.

9. R. T. Gregory, The use of finite segment p-adic arithmetic for exact computation, BIT, Vol. 21, pp. 282-300, September 1978.

10. D. E. Knuth, The Art of Computer Programming 2: Semi-numerical algorithms, Addison-Wesley, Reading, MA, 1980.

11. E. V. Krishnamurthy, On the conversion of Hensel codes to Farey rationals, IEEE Trans. Computers (in press).

12. A. Ya. Khinchin, Continued Fractions, The University of Chicago Press, Chicago, IL, 1964.

13. G. Rodrigue, Parallel Computations, Academic Press, NY, 1982.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE MATRIX INVERSION BASED ON p-ADIC APPROXIMATION		5. TYPE OF REPORT & PERIOD COVERED Techical
		6. PERFORMING ORG. REPORT NUMBER TR-1229
7. AUTHOR(s) E. V. Krishnamurthy		8. CONTRACT OR GRANT NUMBER(s) AFOSR-77-3271
9. PERFORMING ORGANIZATION NAME AND ADDRESS Computer Vision Laboratory, Computer Science Center, University of Maryland, College Park, MD 20742		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 61102F 2304/A2
11. CONTROLLING OFFICE NAME AND ADDRESS Math. & Info. Sciences, AFOSR/NM, Bolling AFB, Washington, DC 20332		12. REPORT DATE November 1982
		13. NUMBER OF PAGES 18
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Parallel computation
Matrix inversion
p-adic approximation

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Newton-Schultz iterative scheme is reformulated in an algebraic setting to compute the exact inverse of a matrix (or the solution of a linear system of equations) over the ring of integers, with a high order of convergence, by using a finite segment p-adic representation of a rational. This method is divergence-free; it starts with the inverse of a given matrix over a finite field (called the priming step) and then iterates successively to construct, in parallel, the p-adic approximants (Hensel Codes) of the rational

DD FORM 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

D

FI

6-